(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年7月14 日 (14.07.2005)

PCT

(10) 国際公開番号
WO 2005/064844 A1

(51) 国際特許分類[7]: H04L 9/08, G09C 1/00

(21) 国際出願番号: PCT/JP2004/019110

(22) 国際出願日: 2004 年12 月21 日 (21.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-433903
2003 年12 月26 日 (26.12.2003) JP
特願2003-433904
2003 年12 月26 日 (26.12.2003) JP
特願2004-023796 2004 年1 月30 日 (30.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 布田 裕一 (FUTA, Yuichi). 大森 基司 (OHMORI, Motoji).

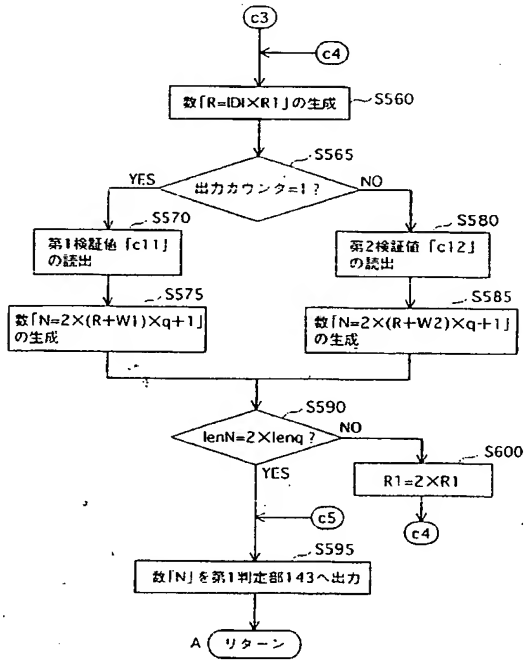
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,

/続葉有/

(54) Title: PRIME CALCULATION DEVICE, METHOD, AND KEY ISSUING SYSTEM

(54) 発明の名称: 素数算出装置及び方法並びに鍵発行システム



S560 GENERATE NUMBER [R = IDI × R1]
S565 OUTPUT COUNTER = 1?
S570 READ FIRST VERIFICATION VALUE [c11]
S580 READ SECOND VERIFICATION VALUE [c12]
S575 GENERATE NUMBER [N = 2 × (R + W1) × q + 1]
S585 GENERATE NUMBER [N = 2 × (R + W2) × q + 1]
S595 OUTPUT NUMBER [N] TO FIRST JUDGMENT UNIT 143
A RETURN

(57) Abstract: There is provided a prime calculation device for calculating a prime and capable of checking whether the prime is generated validly. The prime calculation device generates a disturbing number and multiplies the management identifier by the disturbing number so as to obtain a multiplier R. For w satisfying 2 × W × prime q + 1 = verification value (mod management information), a prime candidate N is calculated by using N = 2 × (multiplier R + w) × prime q + 1. Next, the prime candidate N is judged to be a prime or not. If it is judged to be a prime, the calculated prime candidate N is outputted as a prime.

(57) 要約: 正当に生成されたものであるか否かを確認できる素数を算出する素数算出装置を提供する。 素数算出装置は、乱数を生成し、管理識別子に前記乱数を乗じて乗算値Ｒを算出し、２×ｗ×素数ｑ＋１＝検証値 （ｍｏｄ 管理情報）を満たすｗについて、Ｎ＝２×（乗算値Ｒ＋ｗ）×素数ｑ＋１により、素数候補Ｎを算出する。次に、算出された素数候補Ｎが素数であるか否かを判定し、素数であると判定される場合に、算出された素数候補Ｎを素数として出力する。

WO 2005/064844 A1

ATTACHMENT A

ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。